

A

11/30/99  
JC583 U.S. PTO

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 42390.P7947

Total Pages 2

First Named Inventor or Application Identifier Graunke et al.

Express Mail Label No. EL431684500US

ADDRESS TO: Assistant Commissioner for Patents  
Box Patent Application  
Washington, D. C. 20231

JC542 U.S. PTO  
09/452329  
11/30/99

## APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form  
(Submit an original, and a duplicate for fee processing)
2. X Specification (Total Pages 15)  
(preferred arrangement set forth below)
  - Descriptive Title of the Invention
  - Cross References to Related Applications
  - Statement Regarding Fed sponsored R & D
  - Reference to Microfiche Appendix
  - Background of the Invention
  - Brief Summary of the Invention
  - Brief Description of the Drawings (if filed)
  - Detailed Description
  - Claims
  - Abstract of the Disclosure
3. X Drawings(s) (35 USC 113) (Total Sheets 3)
4. X Oath or Declaration (Total Pages 8)
  - a. X Newly Executed (Original or Copy)
  - b.      Copy from a Prior Application (37 CFR 1.63(d))  
(for Continuation/Divisional with Box 17 completed) (Note Box 5 below)
  - i.      DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5.      Incorporation By Reference (useable if Box 4b is checked)  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6.      Microfiche Computer Program (Appendix)
7.      Nucleotide and/or Amino Acid Sequence Submission  
(if applicable, all necessary)
  - a.      Computer Readable Copy
  - b.      Paper Copy (identical to computer copy)
  - c.      Statement verifying identity of above copies

### ACCOMPANYING APPLICATION PARTS

8. ☐ Assignment Papers (cover sheet & documents(s))
9. ☐ a. 37 CFR 3.73(b) Statement (where there is an assignee)  
☐ b. Power of Attorney
10. ☐ English Translation Document (if applicable)
11. ☐ a. Information Disclosure Statement (IDS)/PTO-1449  
☐ b. Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. ☐ a. Small Entity Statement(s)  
☐ b. Statement filed in prior application, Status still proper and desired
15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☒ Other: Separate Sheet: Certificate of Mailing with Attorney Signature and copy of  
return postcard.  
\_\_\_\_\_  
\_\_\_\_\_

17. If a **CONTINUING APPLICATION**, check appropriate box and supply the requisite information:  
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP)  
of prior application No: \_\_\_\_\_

18. **Correspondence Address**

☐ Customer Number or Bar Code Label \_\_\_\_\_  
(Insert Customer No. or Attach Bar Code Label here)  
or  
☒ Correspondence Address Below

NAME Aloysius T.C. AuYeung, Reg. No. 35,432  
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard  
Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (503) 684-6200 FAX (503) 684-3245

Express Mail Label: EL431684500US

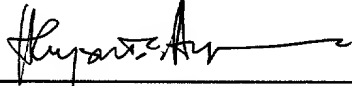
A STREAM CIPHER HAVING A COMBINER FUNCTION WITH STORAGE BASED  
SHUFFLE UNIT

Inventors: Graunke et al.  
Our Reference: 42390.P7947

Respectfully submitted,

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, L.L.P.

Date: 11/30, 1999

  
Aloysius T.G. AuYeung  
Reg. No. 35,432

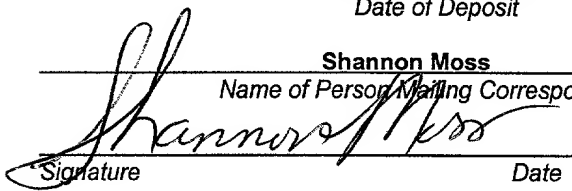
I hereby certify that I am causing this paper or fee to be deposited with the  
United States Postal Service "Express Mail Post Office to Addressee"  
service on the date indicated below and that this paper or fee has been  
addressed to the Assistant Commissioner for Patents, Washington, D.C.  
20231 on:

November 30, 1999

Date of Deposit

Shannon Moss

Name of Person Mailing Correspondence

  
Signature

11/30/99  
Date

EL431684500US

"Express Mail" mailing label number

Serial/Patent No.: not yet assigned

Filing/Issue Date: 11-30-99

Client: Intel Corporation

Title: A STREAM CIPHER HAVING A COMBINER FUNCTION WITH STORAGE BASED  
SHUFFLE UNIT

BSTZ File No.: 42390.P7947

Atty/Secty Initials: ATA/mjt

Date Mailed: 11-30-99

Docket Due Date: \_\_\_\_\_

The following has been received in the U.S. Patent & Trademark Office on the date stamped hereon:

- ☐ Amendment/Response (\_\_\_\_ pgs.)  
☐ Appeal Brief (\_\_\_\_ pgs.) (in triplicate)  
☒ Application - Utility (15 pgs., with cover and abstract)  
☐ Application - Rule 1.53(b) Continuation (\_\_\_\_ pgs.)  
☐ Application - Rule 1.53(b) Divisional (\_\_\_\_ pgs.)  
☐ Application - Rule 1.53(b) CIP (\_\_\_\_ pgs.)  
☐ Application - Rule 1.53(d) CPA Transmittal (\_\_\_\_ pgs.)  
☐ Application - Design (\_\_\_\_ pgs.)  
☐ Application - PCT (\_\_\_\_ pgs.)  
☐ Application - Provisional (\_\_\_\_ pgs.)  
☐ Assignment and Cover Sheet  
☒ Certificate of Mailing \*  
☒ Declaration & POA (8 pgs.) UNSIGNED  
☐ Disclosure Docs & Orig & Copy of Inventor's Signed Letter (\_\_\_\_ pgs.)  
☒ Drawings: 3 # of sheets includes 4 figures

- ☒ Express Mail No.: EL431684500US ☒ Check No. 178  
☐ \_\_\_\_\_ Month(s) Extension of Time Amt: 778  
☐ Information Disclosure Statement & PTO 1449 (\_\_\_\_ pgs.) ☐ Check No. \_\_\_\_\_  
☐ Issue Fee Transmittal Amt: \_\_\_\_\_  
☐ Notice of Appeal  
☐ Petition for Extension of Time  
☐ Petition for \_\_\_\_\_  
☒ Postcard  
☐ Power of Attorney (\_\_\_\_ pgs.)  
☐ Preliminary Amendment (\_\_\_\_ pgs.)  
☐ Reply Brief (\_\_\_\_ pgs.)  
☐ Response to Notice of Missing Parts  
☐ Small Entity Declaration for Indep. Inventor/Small Business  
☒ Transmittal Letter, in duplicate  
☒ Fee Transmittal, in duplicate

☒ Other: \* Separate Sheet: Cert of Mailing w/ Atty Signature and Copy of return Postcard

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

**A Stream Cipher Having  
A Combiner Function With Storage Based Shuffle Unit**

Inventor(s): **Gary L. Graunke  
Carl M. Ellison**

\*Express Mail\* mailing label number EL431684500US

Date of Deposit November 30, 1999

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Signature

Date

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP  
12400 Wilshire Boulevard, 7th Floor  
Los Angeles, California 90025  
(503) 684-6200

"Express Mail" label number EL431684500US

**A Stream Cipher Having A Combiner Function With Storage Based Shuffle Unit**

**BACKGROUND OF THE INVENTION**

5

1. **Field of the Invention**

The present invention relates to the field of cryptography. More specifically, the present invention relates to the robustness of stream ciphers.

10

2. **Background Information**

Cryptographic ciphers can be broadly divided into block ciphers and stream ciphers. Block ciphers cipher a block of plain text into ciphered text by applying multiple successive rounds of transformation to the plain text, using a cipher key. An example of a block cipher is the well known DES cipher. Stream ciphers cipher a stream of plain data into ciphered data by combining the stream of plain data with a pseudo random sequence dynamically generated using a cipher key. An example of a stream cipher is the well known XPF/KPD cipher.

15

Most stream ciphers employ one or more linear feedback shift registers (LFSR). In various applications, it is desirable to employ multiple LFSRs to increase the robustness of a stream cipher. However, employment of multiple LFSRs requires employment of a combiner function to recombine the multiple data bits output by the LFSRs. Most combiner functions known in the art are inefficient in their real estate requirement for hardware implementations. Thus, a robust stream cipher with a more efficient combiner function is desired.

20

25

## SUMMARY OF THE INVENTION

A stream cipher is provided with a first and a second data bit generators to generate in parallel a first and a second stream of data bits. The stream cipher is further provided with a combiner function having a shuffling unit including a storage structure to generate a pseudo random sequence, by combining the first stream of data bits with at least stochastically generated past values of the first stream of data bits, generated by using the second stream of data bits to stochastically operate the storage structure of the shuffle unit to memorize and reproduce the data bits of the first stream.

## BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references  
5 denote similar elements, and in which:

**Figure 1** illustrates an overview of the stream cipher of the present invention, in accordance with one embodiment;

**Figure 2** illustrates a manner in which the LFSRs of **Fig. 1** are initialized, in accordance with one embodiment; and

10 **Figures 3a-3b** illustrate the shuffle unit of **Fig. 1** in further detail, in accordance with two embodiments.

## DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described, and various details will be set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention, and the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention. However, the order of description should not be construed as to imply that these operations are necessarily performed in the order they are presented, or even order dependent. Lastly, repeated usage of the phrase "in one embodiment" does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein a block diagram illustrating the stream cipher of the present invention, in accordance with one embodiment, is shown. As illustrated, stream cipher **100** includes a number of data bit generators **102** and a combiner function **104** coupled to each other as shown. Data bit generators **102** are initialized with an initial vector and a key. Upon initialization, data bit generators **102** are used to generate a number of streams of data bits, and the generated data bit streams are provided to combiner function **104**. Combiner function **104** in turn generates a pseudo random sequence using the provided data bit streams. More specifically, the sequence is generated by modifying one of the provided streams of data bits with at least stochastically selected past values of the stream. The



stochastic selection is effectuated based on the other streams. For the illustrated embodiment, in addition to the stochastically selected past values of the stream, the stream is further modified by the other streams.

As illustrated, data bit generators **102** may be formed with linear feedback shift registers (LFSR), complementary in number to the “capacity” of combiner function **104** (to be explained more fully later). For the illustrated embodiment, data bit generators **102** are formed with five linear feedback shift registers (LFSR) **112-120**. Combiner function **104** is formed with a storage unit based shuffling unit **122** and an XOR function **124**. Storage unit based shuffling unit **122** includes storage locations that can be selectively written into and read from. The number of storage locations included is complementary to the number of LFSRs employed to form data bit generators **102**. For the illustrated 5 LFSR embodiment, storage unit base shuffling unit **122** is equipped with at least 16 storage locations that can be selectively written into and read out of, using 4 of the 5 provided streams of data bits generated by LFSR **112-120**.

Upon initialization with the key and the initial vector, LFSR **112-120** is operated to generate five streams of data bits for combiner function **104**. Shuffling unit **122** shuffles one stream of data bits by stochastically storing the data bits into its storage locations, and at the same time, retrieving the previously stored data bits in the storage locations being written over, in accordance with the data bits of the remaining four streams. The retrieved past values are in turn used by XOR function **124** to modify the same stream of data bits, to generate the pseudo random sequence. For the illustrated embodiment, in addition to the retrieved past values of the stream, the XOR function also uses the other streams, streams generated by LFSR **114-120**, to modify the stream.

As will be appreciated by those skilled in the art, more or less LFSR and storage locations may be used to practice the present invention, as long as their capacities remain complementary to each other. In one embodiment, the five LFSR **112-120** are uneven in length. More specifically, their lengths are 31 bits, 29 bits, 27 bits, 25 bits and 23 bits. Additionally, each LFSR **112, 114, 116, 118** or **120** includes 8 taps. The tap positions are preferably spread out, in one embodiment, accordingly to the following position table:

LFSR	Tap positions
LFSR (31 bit)	31, 25, , 21, 17, 13, 11, 6, 1
LFSR (29 bit)	29, 24, 18, 17, 12, 9, 5, 1
LFSR (27 bit)	27, 23, 19, 15, 11, 7, 4, 1
LFSR (25 bit)	25, 21, 8, 14, 12, 8, 5, 1
LFSR (23 bit)	23, 18, 15, 12, 11, 8, 4, 1

**Figure 2** illustrates a manner in which LFSR **112-120** are initialized with a key and an initial vector, in accordance with one embodiment. For the illustrated embodiment, the initial key is assumed to be 56 bits in size, whereas the initial vector is assumed to be 32 bits in size. Both the initial key as well as the as the initial vectors are sub-divided into 8-bit chunks, i.e.  $\text{Key} = K_6 + K_5 + K_4 + K_3 + K_2 + K_1 + K_0$ , and  $\text{Initial Vector (IV)} = IV_3 + IV_2 + IV_1 + IV_0$  (with  $K_0$  and  $IV_0$  being the least significant bits (LSB)). As illustrated, the 31-bit LFSR is initialized with  $K_0$ , the complement of the LSB of  $K_0$ ,  $K_5$ ,  $K_6$  and a truncated  $K_4$ , whereas the 29-bit LFSR is initialized with  $K_1$ ,  $IV_3$ ,  $K_0$ , the complement of the LSB of  $K_1$ , and a truncated  $K_5$ . Similarly, the 27-bit LFSR is initialized with  $K_2$ ,  $IV_0$ , the complement of the LSB of  $K_2$ ,  $K_1$  and a truncated  $K_6$ , whereas the 25-bit LFSR is initialized with  $K_3$ ,  $IV_1$ , the

complement of the LSB of K3, and K2. Finally, the 23-bit LFSR is initialized with K4, IV2, the complement of the LSB of K4, and a truncated K3. In alternate embodiments, keys and initial vectors of other lengths as well as other segmentation and loading strategies may be employed instead.

5

**Figures 3a-3b** illustrate shuffle unit **122** in further detail in accordance with two embodiments. For the embodiment of **Fig. 3a**, shuffle unit **122** includes memory unit **302** having 16 addressable memory locations **312**, data input port **314**, four write address pins **316**, four read address pins **318** and data output port **320**, thereby allowing the data bits streams generated by the LFSR **114-120** to stochastically control the writing of data bit stream generated by LFSR **112** into memory locations **312** as well as retrieving past values of the data stream previously stored in memory locations **312**. As earlier described, the past values are retrieved from the same storage locations being written into with new data values.

10

15

For the embodiment of **Fig. 3b**, shuffle unit **122** includes memory unit **352** having 16 memory locations **362**, 1 to n de-multiplexor **364**, and n to 1 multiplexor **366** (n being equal to 16 in this case), thereby also allowing the data bits streams generated by the LFSR **114-120** to stochastically control the writing of the data bit stream generated by LFSR **112** into memory locations **352** as well as retrieving past values of the data stream previously stored in memory locations **352**. Again, the past values are retrieved from the same storage locations being written into with new data values.

20

### Epilogue

25

From the foregoing description, those skilled in the art will recognize that many other variations of the present invention are possible. Thus, the present

invention is not limited by the details described, instead, the present invention can be practiced with modifications and alterations within the spirit and scope of the appended claims.

---

## CLAIMS

What is claimed is:

- 1 1. A stream cipher comprising:  
2 a first and a second data bit generator to generate in parallel a first and a  
3 second stream of data bits; and  
4 a combiner function coupled to the first and second data bit generators,  
5 having a shuffle unit including a storage structure, to generate a pseudo random  
6 sequence by modifying the first stream of data bits with at least a stochastic stream  
7 of past values of the first stream of data bits generated by using the second stream  
8 of data bits to stochastically operate the storage structure of the shuffle unit to  
9 memorize and reproduce past values of the first stream.
- 1 2. The stream cipher of claim 1, wherein the combiner function generates the  
2 past values of the first stream of data bits by using the second stream of data bits to  
3 stochastically control writing of the first stream of data bits into storage locations of  
4 the storage structure, and at the same time, retrieving past written values from the  
5 storage locations being written into.
- 1 3. The stream cipher of claim 1, wherein at least one of the first and the second  
2 data bit generator comprises a linear feedback shift register.
- 1 4. The stream cipher of claim 1, wherein the storage structure comprises a  
2 memory unit having a plurality of addressable memory locations, an input port

3 coupled to the first data bit generator, an output port, at least one read address port  
4 and at least one write address port coupled to the second data bit generator.

1 5. The stream cipher of claim 1, wherein the combiner function comprises a 1 to  
2 n de-multiplexor having an input bit line coupled to said first data bit generator, n  
3 output bit lines coupled to the storage structure, and at least one control bit line  
4 coupled to said second data bit generator, where n is an integer greater than 1.

1 6. The stream cipher of claim 1, wherein the combiner function comprises an n  
2 to 1 multiplexor having n output bit lines coupled to said storage structure, an output  
3 bit line, and at least one control bit line coupled to said second data bit generator,  
4 where n is an integer greater than 1.

1 7. The stream cipher of claim 1, wherein the stream cipher further comprises a  
2 third data bit generator coupled to the combiner function to generate a third stream  
3 of data bits for the combiner function, and the combiner function is to further operate  
4 the storage structure to memorize and reproduce past values of the first stream  
5 using the third stream of data bits.

1 8. The stream cipher of claim 7, wherein the stream cipher further comprises a  
2 fourth data bit generator coupled to the combiner function to generate a fourth  
3 stream of data bits for the combiner function, and the combiner function is to further  
4 operate the storage structure to memorize and reproduce past values of the first  
5 stream using the fourth stream of data bits.

1 9. The stream cipher of claim 1, wherein the combiner function further  
2 comprises a XOR function coupled to the first bit data generator and the storage unit  
3 to generate the pseudo random sequence by performing an XOR function on at  
4 least said first stream and its past values.

1 10. A method comprising:  
2 generating in parallel a first and a second stream of data bits;  
3 stochastically generating a stream of past values of the first stream of data  
4 bits using the second stream of data bits; and  
5 generating a pseudo random sequence by combining the first stream of data  
6 bits with at least the stochastically generated stream of past values of the first  
7 stream.

1 11. The method of claim 10, wherein said stochastic generation of a stream of  
2 past values of the first stream of data bits comprises selectively writing the first  
3 stream of data bits into a plurality of storage locations based at least in part on said  
4 second streams of data bits, and at the same time, retrieving past written values of  
5 the first stream of data bits from the storage locations being written into.

1 12. The method of claim 10, wherein said generation of first and second streams  
2 of data bits comprises shifting a first and a second linear feedback shift register in  
3 parallel.

1 13. The method of claim 12, wherein the method further comprises initializing the  
2 first feedback shift register with a first plurality of key segments, and the second

3 linear feedback shift register with a second plurality of key segments and at least  
4 one initial vector segment.

1 14. The method of claim 10, wherein said stochastic generation of past values of  
2 the first stream of data bits comprises applying said first stream of data bits to an  
3 input port of the storage locations, and said second stream of data bits to a read and  
4 a write address port of the storage locations.

1 15. The method of claim 10, wherein said stochastic generation of past values of  
2 the first stream of data bits comprises applying said first stream of data bits to an  
3 input bit line of a 1 to n de-multiplexor, and said second stream of data bits to a  
4 control bit line of the 1 to n de-multiplexor.

1 16. The method of claim 10, wherein said stochastic generation of past values of  
2 the first stream of data bits comprises applying said second stream of data bits to a  
3 control bit line of a n to 1 multiplexor.

1 17. The method of claim 10, wherein said generation of first and second streams  
2 of data bits further comprises generating a third stream of data bits, and said  
3 stochastic generation of past values of the first stream of data bits further uses said  
4 third stream of data bits.

1 18. The method of claim 17, wherein said generation of first and second streams  
2 of data bits further comprises generating a fourth stream of data bits, and said  
3 stochastic generation of past values of the first stream of data bits further uses said  
4 fourth stream of data bits.



1 19. The method of claim 10, wherein the method further comprises performing an  
2 XOR function on said first stream of data bits and at least its past values.

1 20. An apparatus comprising:  
2 first and second data bit generation means for generating in parallel a first  
3 and a second stream of data bits; and  
4 combiner means coupled to the first and second data bit generation means,  
5 including shuffling means having storage means, for generating a pseudo random  
6 sequence, by combining the first stream of data bits with at least a stochastically  
7 generated stream of past values of the first stream of data bits generated by using  
8 the second streams of data bits to stochastically operate the storage means of the  
9 shuffle means to memorize and reproduce past values of the first stream.

1 21. The apparatus of claim 20, wherein the combiner means uses the second  
2 streams of data bits to stochastically control writing of the first data streams into  
3 storage locations of the storage means, and at the same time, retrieving past values  
4 written into storage locations being written into.

ABSTRACT OF THE DISCLOSURE

A stream cipher is provided with a first and a second data bit generators to generate in parallel a first and a second stream of data bits. The stream cipher is further provided with a combiner function having a shuffling unit including a storage structure to generate a pseudo random sequence, by combining the first stream of data bits with at least stochastically generated past values of the first streams of data bits, generated by using the second stream of data bits to stochastically operate the storage structure of the shuffle unit to memorize and reproduce the data bits of the first stream.

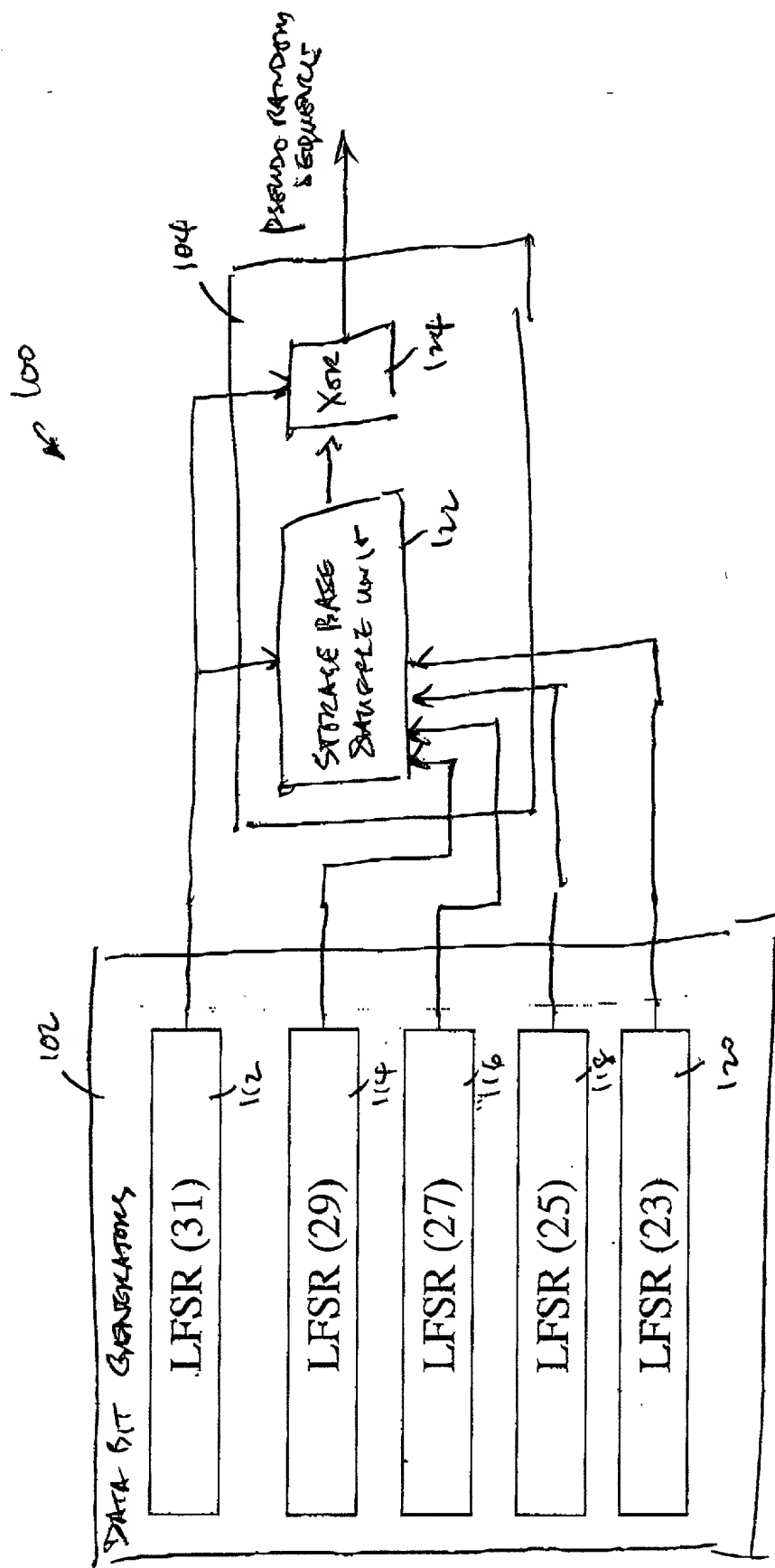


FIG. 1

# Initialization

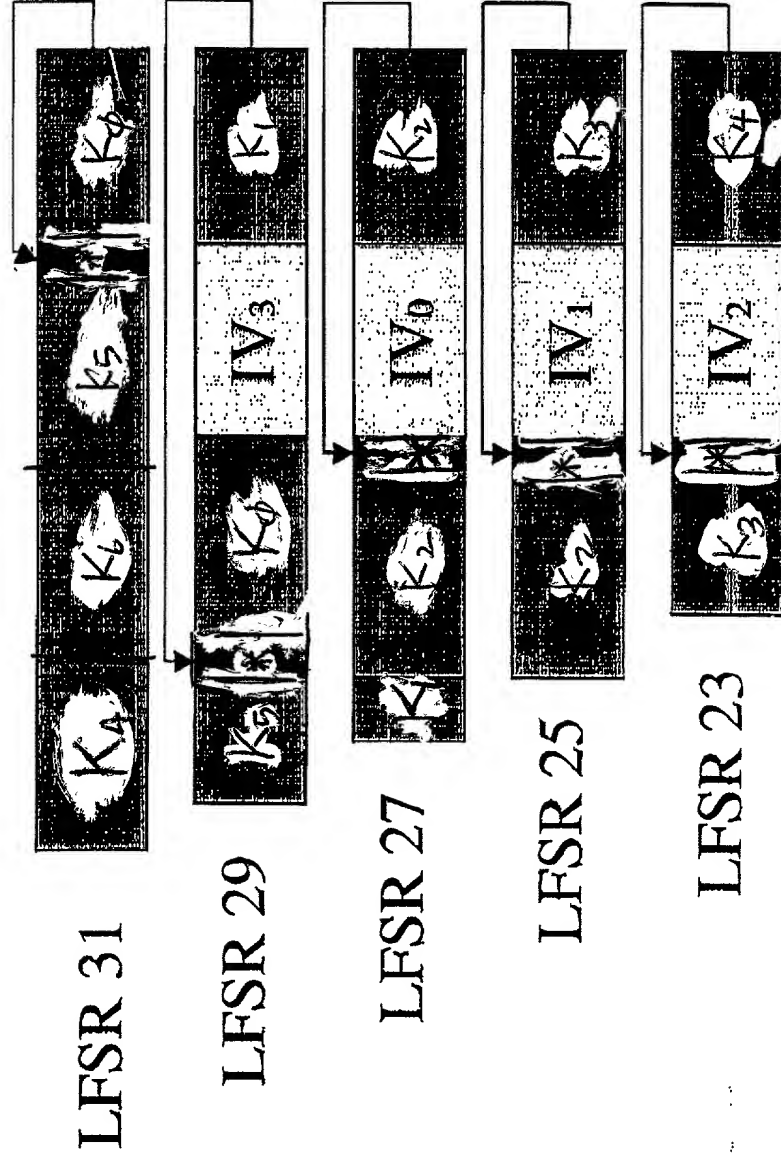


Fig. 2

\* Least significant bit of register is complemented

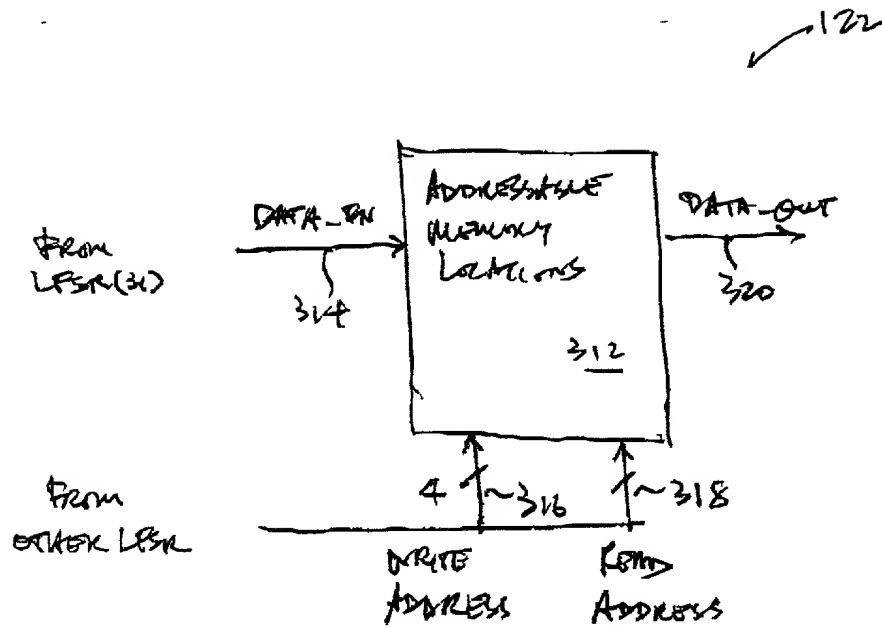


Fig. 3a

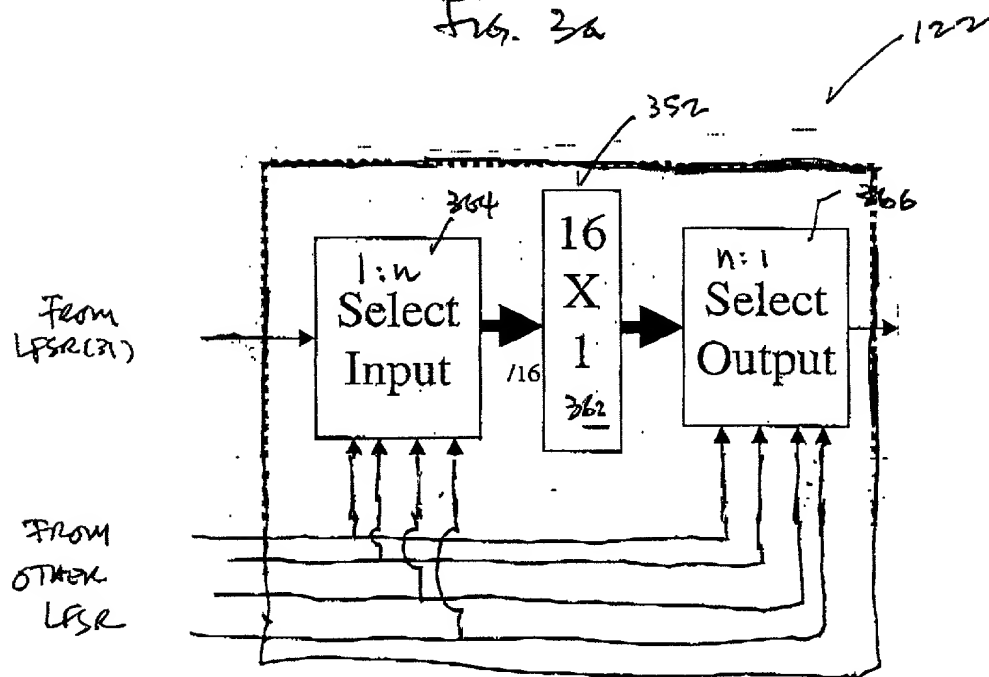


Fig. 3b

**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION**  
**(FOR INTEL CORPORATION PATENT APPLICATIONS)**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**SHUFFLING STREAM CIPHER METHOD AND APPARATUS**

the specification of which

XX is attached hereto.  
\_\_\_\_\_ was filed on \_\_\_\_\_ as  
United States Application Number \_\_\_\_\_  
or PCT International Application Number \_\_\_\_\_  
and was amended on \_\_\_\_\_.  
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority  
Claimed

_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	_____ Yes	_____ No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	_____ Yes	_____ No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	_____ Yes	_____ No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

_____ (Application Number)	_____ Filing Date
_____ (Application Number)	_____ Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

_____ (Application Number)	_____ Filing Date	_____ (Status -- patented, pending, abandoned)
_____ (Application Number)	_____ Filing Date	_____ (Status -- patented, pending, abandoned)

I hereby appoint Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; Amy M. Armstrong, Reg. No. 42,265; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Kent M. Chen, Reg. No. 39,630; Yong S. Choi, Reg. No. P43,324; Thomas M. Coester, Reg. No. 39,637; Roland B. Cortes, Reg. No. 39,152; Barbara Bokanov Courtney, Reg. No. 42,442; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; Richard Leon Gregory, Jr., Reg. No. 42,607; Dinu Gruia, Reg. No. P42,996; David R. Halvorson, Reg. No. 33,395; Thomas A. Hassing, Reg. No. 36,159; Phuong-Quan Hoang, Reg. No. 41,839; Willmore F. Holbrow III, Reg. No. P41,845; George W. Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. No. 42,004; Thinh V. Nguyen, Reg. No. 42,034; Kimberley G. Nobles, Reg. No. 38,255; Babak Redjaian, Reg. No. 42,096; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Anand Sethuraman, Reg. No. P43,351; Charles E. Shemwell, Reg. No. 40,171; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; George G. C. Tseng, Reg. No. 41,355; Lester J. Vincent, Reg. No. 31,460; John Patrick Ward, Reg. No. 40,216; Stephen Warhola, Reg. No. 43,237; Charles T. J. Weigell, Steven D. Yates, Reg. No. 42,242; Reg. No. 43,398; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my attorneys, and James A. Henry, Reg. No. 41,064; Daniel E. Ovanezian, Reg. No. 41,236; Glenn E. Von Tersch, Reg. No. 41,364; and Chad R. Walsh, Reg. No. 43,235; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Cynthia Thomas Faatz, Reg. No. 39,973; Sean Fitzgerald, Reg. No. 32,027; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Jeffrey S. Draeger, Reg. No. 41,000; Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells, Reg. No. P43,256; and Alexander Ulysses Witkowski, Reg. No. P43,280; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.



Send correspondence to Aloysius T.C. Au Yeung, BLAKELY, SOKOLOFF, TAYLOR  
(Name of Attorney or Agent)  
& ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025  
and direct telephone calls to Aloysius T.C. Au Yeung, (503) 264-9174.  
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Gary L. Graunke

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence Hillsboro, OR Citizenship USA  
(City, State) (Country)

Post Office Address 362 NE Hillwood Drive  
Hillsboro, OR 97124-3441

Full Name of Second/Joint Inventor Carl M. Ellison

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence Portland, OR Citizenship USA  
(City, State) (Country)

Post Office Address 1818 NW 28<sup>th</sup> Ave  
Portland, OR 97210-2214

Full Name of Third/Joint Inventor \_\_\_\_\_

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

**INTEL CORPORATION**

Rev. 11/30/98 (D3 INTEL)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

Full Name of Fourth/Joint Inventor \_\_\_\_\_

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

Full Name of Fifth/Joint Inventor \_\_\_\_\_

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

Full Name of Sixth/Joint Inventor \_\_\_\_\_

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

Full Name of Seventh/Joint Inventor \_\_\_\_\_

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

Title 37, Code of Federal Regulations, Section 1.56  
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) Prior art cited in search reports of a foreign patent office in a counterpart application, and
- (2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

- (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
- (2) It refutes, or is inconsistent with, a position the applicant takes in:
  - (i) Opposing an argument of unpatentability relied on by the Office, or
  - (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent

with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

- (1) Each inventor named in the application;
- (2) Each attorney or agent who prepares or prosecutes the application; and
- (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.